一种安全高效的群签名方案

欧海文[1]　雷亚超[2]　王湘南[2]

[1](北京电子科技学院　北京 100070)

[2](西安电子科技大学通信工程学院　陕西 西安 710071)

摘　要　通过对一些基于椭圆曲线的具有前向安全性群签名的研究与分析,提出一种具有前向和后向安全性的高效群签名方案。通过添加随机数的方式打破了公钥状态列表中公钥和私钥的直接联系,规避了被撤销成员联合得出其他成员私钥的风险;设计一个群成员私钥随时间段跨越而自然更新的方案(群管理员的私钥也因应改变),避免以往群成员发生私钥泄漏后需要重新选取密钥对才能保证后续签名安全性的繁琐过程。

关键词　群签名　前向安全性　后向安全性

中图分类号　TP3　　**文献标志码**　A　　DOI:10.3969/j.issn.1000-386x.2020.07.051

A SECURE AND EFFICIENT GROUP SIGNATURE SCHEME

Ou Haiwen[1]　Lei Yachao[2]　Wang Xiangnan[2]

[1](*Beijing Electronics Science and Technology Institute*, *Beijing 100070*, *China*)

[2](*School of Telecommunications Engineering*, *Xidian University*, *Xi'an 710071*, *Shaanxi*, *China*)

Abstract　Through the research and analysis of some forward secure group signatures based on elliptic curve, we propose an efficient group signature scheme with forward and backward security. We broke the direct connection between public key and private key in public key status list by adding a random number, and avoided the risk that the revoked members could jointly obtain the private keys of other members. A scheme was designed to update the private key of group members naturally over time (the private keys of group administrator should be changed accordingly), which avoided the tedious process of re-selecting key pairs to ensure the security of subsequent signatures after the private key leakage of group members.

Keywords　Group signature　Forward security　Backward security

0　引　言

群签名作为一种特殊的数字签名,不仅可以实现对签名者的匿名,在必要的时候还可以实现对签名者的追踪。因此,自 1991 年群签名[1]被提出以来,短时间内就出现了很多经典的群签名方案[2-5],同时随着应用情况和安全性因素的变化,很多改进方案也相应而生[6-7]。为了进一步提高群签名方案的效率和安全性,2015 年白永祥[8]提出了一种高效的群签名方案。2018 年,针对白永祥方案不能抵抗合谋攻击的问题,于璇等[9]基于椭圆曲线上的离散对数问题对白永祥的方案进行了改进,虽然增强了其抗合谋攻击的能力,但是改进方案过于繁琐复杂,执行效率较低。

本文通过对这些群签名方案[8-9]进行深入分析和研究,提出了一个安全性无减弱,但签名长度更短、计算复杂度更低的签名方案。该方案首先通过添加随机数的方式打破了公钥状态列表中公钥和私钥的直接联系,规避了被撤销成员联合得出其他成员私钥的风险。其次,考虑到应用过程中私钥泄露所造成的严重后果,在对一些具有前向安全性群签名方案研究[10-13]的基础上,提出了具有下述特点的群成员和群管理员的密钥更新方案:群成员私钥随时间段跨越而自然更新,群中成员不需要重新修改原始密钥,只要使签名方案进入下一个时间段,就可以成功度过危险期,避免因私钥泄露造成的危害。而且在不知道随机数 r 和 a 的情况

收稿日期:2019-05-23。**欧海文**,教授,主研领域:密码算法的编码、分析与应用。**雷亚超**,硕士生。**王湘南**,硕士生。

下,方案具有前后向安全性,从而减少了群成员反复注册和修改信息的次数,大大增加了方案在应用时的容错性和稳定性。相较于文献[10-13],本文通过在签名过程中将私钥更新方案中的变化量间接传递给群管理员,简化了由于私钥变化所造成的复杂的检验过程,而且还不需要借助第三方的参数。

本文研究改进的群签名方案对当今应用广泛的区块链技术也有重要的意义。因为区块链的去中心和不可篡改特性,使得用户的身份和交易信息一旦泄露将是永久性行为,所以当区块链系统中的用户存在密钥泄露时,就会造成不可挽回的永久性损失。由于本文提出的方案中设置了随时间段变化的私钥更新环节,所以当区块链中用户利用该方案进行交易签名确认时,不仅可以在私钥泄露后保证前面所进行交易的安全性,还可以使用户继续进行安全的交易签名,降低了私钥泄露带来的巨大损失。

1 签名方案

由文献[14]可知,存在满足条件的椭圆曲线可构成 co-GDH 的短签名方案。所以本文利用该理论提出了一种签名长度较短的,具有前向安全性的新的群签名方案。

1.1 系统初始化

选取 $G_1 = <P>$, $G_2 = <Q>$, $|G_1| = |G_2| = p$,其中 $P \in E(F_q)$, $Q \in E(F_{q^\alpha})$。由文献[9]可知,存在对应的非退化的双线性映射 $e: G_1 \times G_2 \to G_T$, $H: \{0,1\}^* \to G_1$, $H_1: \{0,1\}^* \to Z_p$,同构映射 $\psi: G_2 \to G_1$。

对于 GM:取 $x_0 \in_R Z_p$,计算 $Y = x_0 Q \in G_2$,其中 x_0 为群管理员私钥,Y 为公钥。故群公共参数为 $\{p, P, Q, G_1, G_2, e, H, \psi\}$,群公钥为 Y。

1.2 成员加入

(1) 对于 u_i, u_i 取 $x_{i,0}, r_i \in_R Z_p$,计算 $y_i = x_{i,0} Q \in G_2$, $K_i = r_i H(ID_i)$, $L_i = r_i Q$,然后将 (ID_i, y_i, K_i, L_i) 发送给 GM。其中 ID_i 代表成员 u_i 的现实身份信息。

(2) 收到 (ID_i, y_i, K_i, L_i) 后,GM 先验证等式 $e(K_i, Q) = e(H(ID_i), L_i)$ 是否成立,确认 ID_i 的有效性。即:

$$e(K_i, Q) = e(r_i H(ID_i), Q) = e(H(ID_i), r_i Q) = e(H(ID_i), L_i)$$

若成立,计算:

$$M_i = e(x_0, y_i) \quad N_i = a_i Q \quad y'_i = y_i + N_i$$

将 (M_i, N_i, y'_i) 发送给 u_i,并存储 ID_i、y'_i、N_i,其中 ID_i、y'_i,以及时戳 $Time$ 构成公开的公钥列表 PKSL,见表 1。

表 1 PKSL 表

ID_i	y'_i	$Time_{i\text{-start}}$	$Time_{i\text{-end}}$
u_1	$y'_1 = y_1 + N_1$	$Time_{1\text{-start}}$	$Time_{1\text{-end}}$
⋮	⋮	⋮	⋮

(3) 成员 u_i 收到 (M_i, N_i, y'_i) 后,验证等式 $M_i = e(x_{i,0}, Y)$, $N_i = y'_i - y_i$ 是否都成立。若成立,则接受 y'_i 为公钥,私钥为 $x_{i,0}$。

1.3 成员密钥更新

成员密钥泄露在签名中往往会造成严重后果,近年来,为了降低密钥泄露所造成的损失,陆续提出了前向安全、入侵容忍和密钥隔离等技术。这些方法都是以密钥更新为基础。其中密钥隔离技术需要借助协助器进行密钥的更新,而且每次更新都是相互独立的,这将会大幅增加通信成本以及对通信安全性的要求。本文方案主要采用前向安全技术,即通过利用一个单向函数进行密钥的更新。即:

(1) 将整个有效时间划分为若干个时间段 1,2,…,L。

(2) 在第 j 阶段,设群成员 u_i 的密钥为 $x_{i,j}$,群管理员密钥为 x_j,则第 $j+1$ 阶段的密钥为:

$$x_{i,j+1} = x_{i,j} + H_1(r_i P \| j+1) - H_1(r_i P \| j)$$

$$x_{j+1} = x_j + pH_1(aP \| j+1)$$

式中:r_i 为 u_i 在申请加入群时选取的随机数,$a \in_R Z_p$ 为固定常数。

(3) 在计算出第 $j+1$ 阶段的密钥后,立即删除第 j 阶段密钥。

1.4 消息签名

群成员 u_i 对于消息 M:

(1) 成员 u_i 首先根据 $Time$ 判断所处的时间段,设为第 j 时间段,计算 $h_1 = H_1(r_i P \| j)$, $h_2 = H_1(r_i P \| 0)$, $h_0 = h_1 - h_2$, $x_{i,j} = x_{i,0} + h_1 - h_2$;其次取 $b_i \in_R Z_p$,计算 $T_i = H(M \| Time \| Q \| b_i Q)$, $V_i = b_i - T_i x_{i,j}$,然后将 $(y'_i, M, Time, T_i, V_i, h_0)$ 发送给群管理员 GM。

(2) GM 首先由 y'_i 值查找 PKSL 表,看其是否为有效值;若有效,根据对应的 N_i 值,验证等式 $T_i = H(M \| Time \| Q \| (V_i Q + T_i(y'_i - N_i + h_0 Q)))$ 是否成立,从而判断其是否为群中合法成员;若成立,则 GM 存储 T_i, V_i 构成追踪列表,同时根据 $Time$ 判断对应的时间段,并计算此时私钥 x_j 及 $c = x_j T_i$,然后将 c 发送给成员 u_i;

若不成立,则拒绝签名请求。追踪列表如表 2 所示。

表 2　追踪列表

ID_i	T_i	V_i
u_1	$T_1 = H(M \parallel Time \parallel Q \parallel b_1 Q)$	$V_1 = b_1 - T_1 x_{1,j}$
⋮	⋮	⋮

(3)成员 u_i接收到 c 后,验证 $e(c,Q) = e(T_i,Y)$ 是否成立,若成立$(c,Time,T_i,V_i)$即为群成员 u_i对于消息 M 的签名。

1.5　签名验证

验证者在接收到签名$(c,Time,T_i,V_i)$后,验证$e(c,Q) = e(T_i,Y)$是否成立,若成立,则接受$(c,Time,T_i,V_i)$为群成员 u_i对于消息 M 的正确的群签名。

1.6　签名打开

关于签名$(c,Time,T_i,V_i)$产生矛盾分歧时,群管理员可以通过查询追踪列表中对应的 T_i、V_i追踪到该签名的签名人 u_i的身份,并给出 $T_i = H(M \parallel Time \parallel Q \parallel (V_i Q + T_i(y'_i - N_i + h_0 Q)))$,证明该签名确实是群成员 u_i产生的。

1.7　成员撤销

由上面叙述可知,群签名是由群成员与群管理员联合产生的。所以,当需要撤销某个群成员时,只需将公开的 PKSL 表中对应的公钥 y'_i的 $Time_{i\text{-end}}$修改为当时的时间,并且在签名时拒绝其签名请求即可。反之,如果某个公钥一直有效,则可以将对应的 $Time_{i\text{-end}}$取个足够大的值,如 2999 年 12 月 30 日等。不过,撤销成员的再次启用则需要重新申请,才能获得合法的群成员身份。

2　正确性与安全性分析

2.1　正确性分析

与文献[9]一样,该方案中的系统建立以及签名过程也存在管理员与成员双向验证身份的过程。

(1) 成员加入过程成员与管理员身份的验证。u_i接收到 GM 发送的(M_i,N_i,y'_i)。首先,通过双线性映射的性质验证 $M_i = e(x_0,y_i) = e(x_{i,0},Y)$,证明确实是群管理员后才接受发送来的$(M_i,N_i,y'_i)$。其次,通过 $N_i = y'_i - y_i$确认 N_i的有效性。

(2) 签名过程中群管理员和成员互验身份。签名是由群管理员和群中成员 u_i联合产生的。一方面,群管理员在接收到群成员发送来的$(y'_i,M,Time,T_i,V_i,h_0)$后,首先根据 PKSL 表判断 y'_i是否在有效时间内,其次核实成员身份。即验证 $T_i = H(M \parallel Time \parallel Q \parallel (V_i Q + T_i(y'_i - N_i + h_0 Q)))$是否成立,若成立,则证明发送方确为群中成员 u_i和$(y'_i,M,Time,T_i,V_i,h_0)$的有效性。另一方面,群中成员 u_i在接收到群管理员发送的 c 后,通过双线性映射的性质验证 $e(c,Q) = e(T_i,Y)$是否成立,若成立,证明 c 确实是群管理员产生的有效值。

(3) 私钥更新的迭代。对于群中成员的私钥更新方案,即:

因为　$x_{i,j+1} = x_{i,j} + H_1(r_i P \parallel j+1) - H_1(r_i P \parallel j)$

所以　$x_{i,j+1} = x_{i,j-1} + H_1(r_i P \parallel j) - H_1(r_i P \parallel j-1) + H_1(r_i P \parallel j+1) - H_1(r_i P \parallel j) =$

$x_{i,j-1} + H_1(r_i P \parallel j+1) - H_1(r_i P \parallel j-1) =$

⋮

$x_{i,0} + H_1(r_i P \parallel j+1) - H_1(r_i P \parallel 0)$

对于群管理员第 $j+1$ 阶段私钥:

$$x_{j+1} = x_j + pH_1(aP \parallel j+1)$$

因为　$|G_2| = p, G_2 = <Q>$

所以　$x_{j+1} Q = x_j Q$

由上述推导过程可知,在不泄露随机数 r_i的情况下,群成员私钥更新方案既具有前向安全性,还具有后向安全性。而对于群管理员,在不泄露随机数 a 的情况下,满足前向安全性,而且在整个群管理员初始密钥有效的过程中,群公钥不发生改变。

(4) 签名的正确性。首先验证签名$(c,Time,T_i,V_i)$中的 c 的正确性,证明签名过程确实有群管理员参与。即验证:$e(c,Q) = e(x_j T_i,Q) = e(T_i,x_j Q) = e(T_i,Y)$。其次,验证 T_i的正确性,即:

$T_i = H(M \parallel Time \parallel Q \parallel b_i Q) =$

$H(M \parallel Time \parallel Q \parallel (V_i Q + T_i(y'_i - N_i + h_0 Q)))$

故只需验证 $b_i Q = V_i Q + T_i(y'_i - N_i + h_0 Q)$。

因为　$V_i = b_i - T_i x_{i,j}$

所以　$b_i Q = (V_i + T_i x_{i,j}) Q = V_i Q + T_i x_{i,j} Q =$

$V_i Q + T_i(x_{i,0} + h_1 - h_2) Q =$

$V_i Q + T_i(x_{i,0} Q + h_0 Q) =$

$V_i Q + T_i(y'_i - N_i + h_0 Q)$

通过上述几个方面的分析,证明了本文所提方案的正确性。

2.2　安全性分析

根据群签名的安全性要求,本文将从以下几个方面论述本文方案的安全性。

(1) 匿名性。接收到签名$(c,Time,T_i,V_i)$后,验证者只是验证$e(c,Q) = e(T_i,Y)$是否成立来决定是否接受该签名,其中只用到了群管理员 GM 的公钥 Y,并

没有涉及群成员 u_i的信息。所以,本方案满足匿名性。

(2) 抗合谋性。首先,本方案基于椭圆曲线离散对数问题的难解性,一方面使群管理员 GM 无法获知群成员的私钥;另一方面还通过添加随机数 N_i的方式,使被撤销成员无法根据 PKSL 表中的公钥 y'_i和各自的私钥,得出其他成员的私钥。其次,本方案通过先验证群成员身份,再由群成员与管理员合作产生签名的形式,加强了签名过程中成员与管理员间的联系,避免了群中成员合谋产生无法追踪的签名。最后,群中所有成员以及管理员 GM 的私钥都完全保密,且互相无关。所以,该方案在抗合谋性方面强于之前签名[8-9]。

(3) 追踪性。接收到签名$(c, Time, T_i, V_i)$后,群管理员 GM 可直接根据 T_i、V_i值查找追踪列表,从而追踪到该签名者的身份信息,实现追踪的目的。

(4) 不可伪造性。由对消息 M 的签名过程可知,签名$(c, Time, T_i, V_i)$由群管理员与群成员 u_i联合生成。其中 $T_i = H(M \| Time \| Q \| (V_iQ + T_ix_{i,j}Q))$,$c$ 则需要满足 $e(c,Q) = e(x_jT_i, Q) = e(T_i, Y)$。因此,只有知道群管理员和群成员私钥 x_j和 $x_{i,j}$才能伪造出符合条件的签名。而由椭圆曲线上的离散对数难解性及 Hash 函数 H 的单向陷门性可知,在所有成员私钥都完全保密的情况下,其他人是无法由 c、T_i、V_i、Y、y'_i得出私钥的。所以,该方案满足不可伪造性。

(5) 不可关联性。对任意消息 M 的签名$(c, Time, T_i, V_i)$,其中 $T_i = H(M \| Time \| Q \| b_iQ)$,$V_i = b_i - T_ix_{i,j}$,$c = x_jT_i$,$b_i \in_R Z_p$,$Time$ 是群成员准备进行签名时从可信时间戳机构获得的时间。所以可知签名中的所有成员都是随机的不涉及签名成员信息的,满足不可关联性。

(6) 防陷害性。由上述签名过程可知群管理员和群成员都不能代替他人产生有效的签名。因为无论是群管理员还是群中成员都有秘密保存的私钥,在其不暴露的情况下,该方案都是满足防陷害性的。而且,由 $T_i = H(M \| Time \| Q \| b_iQ)$,$V_i = b_i - T_ix_{i,j}$可知只有知道私钥 $x_{i,j}$的成员才能产生符合 $T_i = H(M \| Time \| Q \| (V_iQ + T_iy_i + h_0Q))$的 T_i、V_i,故群中成员可通过验证 T_i、V_i的值来防止群管理员冒充自己伪造签名,同时证明群管理员的不可信。

(7) 前向安全性。该签名方案通过构建不改变初始公钥的密钥更新方案,在不同阶段产生不同的私钥值,而且由 Hash 函数的单向性可知,在不知道随机数 r_i和 a 情况下,无法由当前密钥获取之前的密钥。所以即使当前的私钥泄露或丢失,前面阶段所产生的签名仍然是安全的,可被验证的。

(8) 后向安全性。由群成员的私钥更新方案可知,在不知道随机数 r_i的情况下,无法从当前密钥推之前和之后的密钥。故在群成员当前密钥泄露时,不需要重新选取初始密钥,只需过渡到下一阶段,即可进行安全的签名,避免因私钥泄露造成危害。

3 效率分析

文献[9]基于白永祥方案提出了一种椭圆曲线上的高效安全的实现方案。将本文方案与文献[9]方案从成员加入签名验证的计算复杂度进行比较。综合两个签名方案可知,方案中的主要操作是椭圆曲线上的乘法、双线性映射的计算以及 Hash 函数的计算,所以本文主要考虑这三种主要操作的数目来衡量签名方案效率。计算复杂度如表 3 所示。

表 3 计算复杂度对比表

方案	操作	乘法	双线性映射	Hash 函数
文献[9]	成员加入	8	9	1
	签名	6(1 个幂)	2	3
	验签	2(1 个幂)		1
本文	成员加入	6	4	3
	签名	5	2	2
	验签		2	

由表 3 可知,在保持同样安全性的前提下,本文所提方案的效率远高于文献[9]中方案,而且签名长度也短。同时在实现签名的前向安全性方面,本文方案中设计的密钥更新方案较文献[10-13]也更加简洁,而且还能实现后向安全性。

4 结 语

本文通过对以往的群签名方案进行分析和研究,主要基于文献[9]提出了一个具有前/后向安全性的高效的群签名方案。首先,通过以 $y'_i = x_{i,j}Q + N_i$作为私钥 $x_{i,j}$所对应的公钥值,规避了被撤销成员联合得出其他成员私钥的可能性。其次,在保证方案安全性要求的前提下,简化了签名过程,缩短了签名的长度,并且针对群管理员和群中成员设计了不同的密钥更新方案,使方案具有了前后向安全性。最后,由整个签名过程和组成成分可知,在应用时还可根据需要将多个群成员的签名聚合成一个签名,即:$T = T_1 + T_2 + \cdots + T_k$,$c = xT = xT_1 + xT_2 + \cdots + xT_k = c_1 + c_2 + \cdots + c_k$。这些特

(下转第 328 页)

在溯源信息上链频率固定的情况下,针对不同的溯源信息量规模,上链响应时间变化如图 5 所示,随着信息量规模增大,单位信息响应时间基本保持不变。

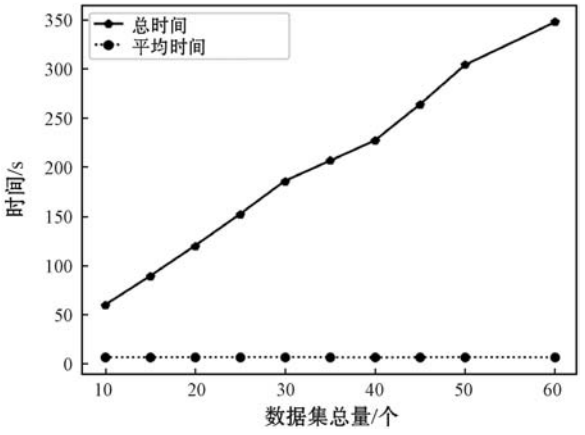

图 5 不同数据量对应响应时间变化

由实验结果可以看出,基于区块链的农产品安全可信溯源应用系统在不同规模溯源信息及不同请求频率下具有高可用性和稳定性,单位信息上链响应平均时间在秒级,具有可扩展性。

5 结 语

本文研究了将区块链技术应用于品牌农产品溯源的一体化应用体系,解决中心化溯源系统信任度低和系统安全的问题,品牌农产品溯源链分布式、不可篡改和共识验证等特性提升了系统的安全性和可信任度。从溯源信息上链和响应时间方面对去中心化溯源系统进行了仿真,结果表明基于区块链的强信任溯源系统具有高可用性和稳定性,且在分布式溯源数据上链可扩展性等方面表现良好。下一步将通过对溯源链细节进行优化,提升不同场景下的系统整体性能表现。

参 考 文 献

[1] 刘耀宗,刘云恒. 基于区块链的 RFID 大数据安全溯源模型[J]. 计算机科学,2018,45(11A):367 - 368,381.

[2] 何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1 - 7,15.

[3] 李静元,范祥辉,王颖. 基于区块链的共享经济隐私保护机制的设计[J]. 计算机应用与软件,2019,36(1):296 - 301.

[4] 杨慧琴,孙磊,赵西超. 基于区块链技术的互信共赢型供应链信息平台构建[J]. 科技进步与对策,2018,35(5):21 - 31.

[5] 钱卫宁,邵奇峰. 区块链与可信数据管理:问题与方法[J]. 软件学报,2018,29(1):150 - 159.

[6] 宋焘谊,赵运磊. 区块链共识算法的比较研究[J]. 计算机应用与软件,2018,35(8):1 - 8.

[7] 陶启,崔晓晖,赵思明,等. 基于区块链技术的食品质量安全管理系统及在大米溯源中的应用研究[J]. 中国粮油学报,2018,33(12):110 - 118.

[8] 宋远方,冯绍雯,宋立丰. 互联网平台大数据收集的困境与新发展路径——基于区块链理念[J]. 中国流通经济,2018,284(5):5 - 13.

[9] 紫琳. 中国首个安全食品区块链溯源联盟成立[J]. 中国食品,2018(1):173.

(上接第 312 页)

性设计将会更易于本文方案的实际应用,尤其是对于现在应用广泛的区块链技术。下一步,我们将会注重研究群签名的实际应用。

参 考 文 献

[1] Chaum D, Heyst E V. Group signatures [C]//Advances in Cryptology—EUROCRYPT'91, 1991: 257 - 265.

[2] Camenisch J, Stadler M. Efficient group signature schemes for large groups [C]//Advances in Cryptology—CRYPTO'97, 1997: 410 - 424.

[3] Camenisch J, Michels M. A group signature scheme based on an RSA-variant [EB/OL]. 1998. Http://citeseer. nj. nec. com/camenisch98group. html.

[4] Ateniese G, Camenisch J, Joye M, et al. A practical and provably secure coalition-resistant group signature scheme, Advances in Cryptology—CRYPTO 2000, 2000: 255 - 270.

[5] 李凤银,禹继国,鞠宏伟. 一种基于 RSA 的群签名方案[J]. 计算机工程与设计,2006,27(16):2955 - 2957.

[6] 姜燕. 基于 RSA 的群签名方案的缺陷及改进方案[J]. 计算机工程与设计,2008,29(7):1655 - 1657,1671.

[7] 朱莹,蔡光兴. 一种基于 RSA 群签名方案的安全性分析及改进[J]. 湖北工业大学学报,2009,24(1):68 - 70,73.

[8] 白永祥. 一种高效群签名方案的设计与分析[J]. 通信技术,2015,48(2):214 - 218.

[9] 于璇,侯书会. 一种高效安全的群签名方案[J]. 通信技术,2018,51(2):413 - 418.

[10] 张晓琳. 前向安全的群签名研究[D]. 青岛:青岛大学,2016.

[11] 韩嫣. 具有前向安全性的动态属性群签名研究[D]. 武汉:武汉理工大学,2017.

[12] 王硕,程相国,陈亚萌,等. 前向安全的群签名方案[J]. 青岛大学学报(自然科学版),2017,30(3):35 - 39.

[13] 王越,程相国,王戌琦. 基于双线性对的密钥隔离群签名方案研究[J]. 信息网络安全,2018,18(6):61 - 66.

[14] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing[C]//7th International Conference on the Theory and Application of Cryptology and Information Security,2001: 514 - 532.